PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Toni MÄKI et al. Group Art Unit: Unassigned

Application No.: New Application Examiner: Unassigned

Filed: August 25, 2003 Attorney Dkt. No.: 60282-00091

For: MULTIMEDIA COMPONENT INTERCEPTION IN A GATEWAY GPRS SUPPORT NODE (GGSN)

CLAIM FOR PRIORITY UNDER 35 USC § 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450 August 25, 2003

Sir:

The benefit of the filing dates of the following prior foreign applications filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

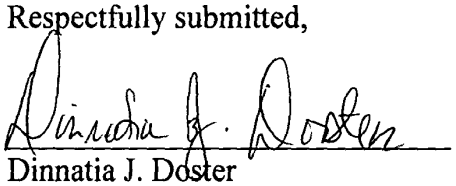
Patent Application No. 03011271.8 filed on May 16, 2003 in Europe.

In support of this claim, a certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Please charge any fee deficiency or credit any overpayment with respect to this paper to Counsel's Deposit Account No. 50-2222.

Respectfully submitted,



Dinnatia J. Doster
Registration No. 45,268

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DJD:cct

Enclosure: Priority Document (1)

Europäisch s Patentamt	European Patent Office	Office uropé n des brevets

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03011271.8

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03011271.8
Demande no:

Anmeldetag:
Date of filing: 16.05.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Nokia Corporation
Keilalahdentie 4
02250 Espoo
FINLANDE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Multimedia component interception in GGSN

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04Q7/38

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

TBK TIEDTKE - BÜHLING - KINNE & PARTNER (GbR)

TBK-Patent POB 20 19 18 80019 Münch n

Patentanwälte
Dipl.-Ing. Reinhard Kinne
Dipl.-Ing. Hans-Bernd Pellmann
Dipl.-Ing. Klaus Grams
Dipl.-Ing. Aurel Vollnhals
Dipl.-Ing. Thomas J.A. Leson
Dipl.-Ing. Dr. Georgi Chivarov
Dipl.-Ing. Matthias Grill
Dipl.-Ing. Alexander Kühn
Dipl.-Ing. Rainer Böckelen
Dipl.-Ing. Stefan Klingele
Dipl.-Chem. Stefan Bühling
Dipl.-Ing. Ronald Roth
Dipl.-Ing. Jürgen Faller
Dipl.-Ing. Hans Ludwig Trösch
Rechtsanwälte
Michael Zöbisch

US 38447

May 16, 2003

NOKIA CORPORATION

Espoo, Finland

„MULTIMEDIA COMPONENT INTERCEPTION IN GGSN"

Dresdner Bank München Kto. 3939 844 BLZ 700 800 00
Deutsch Bank München Kto. 286 1060 BLZ 700 700 10
Postbank München Kto. 67043 804 BLZ 700 100 80
Mizuho Corp. Bank Düsseldorf Kto. 8104233007 BLZ 300 207 00
UFJ Bank Limited Düsseldorf Kto. 500 047 BLZ 301 307 00
/RS218

Telefon: +49 89 544690
Telefax (G3): +49 89 532611
Telefax (G3+G4): +49 89 5329095
E-Mail: postoffice@tbk-patent.de
Internet: http://www.tbk-patent.de
Bavariaring 4-6, 80336 München

TITLE: MULTIMEDIA COMPONENT INTERCEPTION IN GGSN

Field of the invention

This invention relates to a method and a system for intercepting sessions.

Background of the invention

3GPP (Third Generation Partnership Project) Release 5 and Release 6 standards (defined in 3GPP TS 23.228 V5.7.0/6.1.0, for example) define IP (Internet Protocol) Multimedia Core Network Subsystem (IMS). IMS provides users IP based multimedia services like voice over IP, for example. Operators benefit from IMS as services offered traditionally in circuit switched and packet switched networks can be converged into one network using one technology.

IP Multimedia Core Network Subsystem uses GPRS (General Packet Radio Service) as an underlying access and bearer technology (3GPP TS 22.060 V5.2.0). GPRS provides mobile hosts connectivity to packet-based networks like Internet or company intranets. It does this by introducing two network elements, GPRS Support Nodes, and IP based packet core network. Serving GPRS Support Node (SGSN) takes care of terminal mobility, security operations and access control. Gateway GPRS Support Node (GGSN) acts as a gateway providing internetworking with packet data networks. User data is carried between SGSN and GGSN in tunnel provided by GTP (GPRS Tunnelling Protocol) tunnelling protocol. PDP (Packet Data Protocol) context defines the tunnel between SGSN and GGSN, and references to the access point that defines how the user data packets are handled at the GGSN and beyond. For example,

they might be further tunnelled to an intranet. In this description PDP context and the tunnel through GPRS core network are treated as synonyms.

Sessions in IMS are created using SIP (Session Initiation Protocol, as defined in IETF RFC 3261, for example). IMS contains a dedicated network element, CSCF (Call Session Control Function) that handles SIP signalling. IMS level session data is stored in the CSCFs and is not visible to GPRS. To an IMS level session there is associated one or more media components (also known as media streams). One media component is comprised of packets belonging to the same stream defined by either IPv6 (Internet Protocol version 6) flow label or quintuple containing source address, destination address, source port, destination port used protocol. Media components are carried inside a PDP context. One PDP context may carry several media components. In 3GPP Release 5 one PDP context may carry the media components of only one IMS level session. In 3GPP Release 6 one PDP context may carry media components of several IMS level sessions.

In most of the countries operators are under an obligation to provide authorities an access to the information exchanged between communicating parties in a telecommunications network. Implementing lawful interception and delivering the intercepted data might be a precondition for a license to operate a commercial network. Obligation to provide lawful interception ability to authorities applies also to IP Multimedia Core Network Subsystem. Lawful interception is specified by 3GPP standards TS 33.106 V5.1.0, TS 33.107 V5.5.0 and TS 33.108 V5.3.0/6.1.0, for example.

In GPRS the lawful interception is based on one of the following user identities: IMSI (International Mobile Subscriber Identity), MSISDN (Mobile Subscriber International ISDN Number) or IMEI (International Mobile Station Equipment Identity). The interception is applied to signalling and to the actual user data carried in PDP context.

According to 3GPP TS 33.106 V5.1.0, the lawful interception in IMS is based on SIP URL (Uniform Resource Locator). Using this SIP URL the IRI (Interception-Related Information) data from IMS level can be intercepted. To be able to intercept communication content (CC), GPRS level interception is needed. This is accomplished by interworking of CSCF and GGSN. After a signalling exchange, the CSCF knows the PDP context identification used in GPRS network and it can deliver the information to an ADMF (Administration Function). The ADMF may then activate interception in GPRS level targeted on appropriate PDP context(s).

In 3GPP Release 6 one PDP context may carry media components of several IMS level sessions. It is possible, that in the network there will appear such a set-up, where wrong user data gets intercepted by accident. This kind of unauthorised interception is illegal and cannot be allowed to appear in IMS.

The capture of wrong user data happens in a following set-up, which is illustrated in Fig. 1: Interception happens in a local network, Network 1. A remote party, Subscriber A (UE A), belonging to a remote network, Network 2, is intercepted in the local network, Network 1. Subscriber B (UE B), to whom the Subscriber A is calling, has another on-going IMS level session with a

Subscriber C. Both of these two sessions (A - B session, session 1, and B - C session, session 2) are carried over one PDP context from UE of subscriber B to GGSN in local network. Because GPRS level interceptions currently capture all the data carried by a PDP context, also the media component of session between Subscriber B and Subscriber C gets intercepted. This should not occur since only subscriber A is to be intercepted and the (accidental) interception of the session 2 between subscribers B and C is illegal.

It is noted that in 3GPP Release 5 this set-up is not possible as PDP context can carry the media components of only one IMS level session, as described above.

However, in 3GPP Release 6 and similar configurations in which more than one session can be included in one PDP context, this is a serious problem, since in this case interception can likely become illegal.

Summary of the invention

Thus, the object underlying the present invention resides in solving the above problem and to provide a method and a network system by which reliably only those sessions are intercepted which are intended to be intercepted.

This object is solved by a method for intercepting sessions, comprising the steps of

identifying a packet of a session to be intercepted based on media component information of the session, and,

if the packet to be intercepted is identified, providing duplicated packets of the session to an interception management element.

Alternatively, this object is solved by a system for intercepting sessions comprising an intercepting node and an intercepting management element, wherein

the intercepting node is adapted to identify a packet of a session to be intercepted based on media component information of the session, and to provide duplicated packets of the session to the interception management element if the packet to be intercepted is identified.

Thus, according to the invention, instead of capturing the traffic carried in a PDP context, the traffic carried in a media component is captured. This provides a more fine-grained interception where only the traffic meant to be intercepted gets captured and forwarded to an interception management element (e.g., LEA (Law Enforcement Agency)).

Hence, a case in which a second session not to be intercepted is accidentally intercepted can reliably be avoided, since the identification based on the media component information provides a more reliable basis than a PDP context.

Preferably, the media component interception can be performed in GGSN as it handles the IP header of the user data. SGSN forwards this IP header transparently.

The media component information may comprise a multimedia level session identification and a control level media component identification associated to the multimedia level session identification. For example, the multimedia level session identification may be an IMS level session identification.

The multimedia level session identification may comprise an authorisation token, or may comprise a multimedia charging identifier (ICID, IMS Charging Identifier).

The control level media component identification may comprise a flow identifier, as defined in 3GPP TS 29.207 V5.2.0, Annex C, for example.

The media component information may comprise user level media component information.

Furthermore, before performing the actual interception (identifying and providing packets to the interception management element), an activation of the interception may be performed, in which the media component information are obtained from a session initiating procedure in which a target to be intercepted is participating. Thus, the necessary information can easily be provided to the intercepting node and the like. The activation may be performed by a network control element such as an Administration Function (ADMF), for example.

On activating the interception, the media component information may be obtained from user plane data. That is, in this case it can be secured that the traffic to be intercepted belongs to a user the communication of which is to be intercepted. For example, the media component information are obtained from session establishment messages during set-up of a session and negotiating a media component.

Alternatively, upon providing intercepted data to the intercepting management element, data not to be intercepted may be filtered out. In this case, it is

possible to intercept the whole traffic, but the data which is not to be intercepted is filtered out, so that this data (e.g., another media component) is not forwarded to the interception management element. Hence, an illegal interception can reliably prevented.

The filtering may be performed based on media component information or may be based on charging identifiers. For example, such a charging identifier may be a IMS charging ID (ICID). The GPRS Charging ID or IMSI may be used to activate the interception, which then delivers the whole traffic. The data not to be intercepted can than be filtered out by using media component information.

The filtering may be performed in the intercepting node such as SGSN or GGSN, for example, or, alternatively, the filtering may be performed in a separated node. Such a separated node may be a Delivery Function DF3, for example.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a situation according to the prior art, in which an illegal interception may accidentally occur,

Fig. 2 shows a flowchart illustrating the principle of the invention,

Fig. 3 illustrates activation of interception of a media component MC2 according to a first embodiment of the invention,

Fig. 4 shows a signalling flow of the activation of the interception according to the first embodiment,

Fig. 5 illustrates the provision of content of communication carried in the media component MC2 according to the first embodiment, and

Fig. 6 illustrates a second embodiment of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following, preferred embodiments are described by referring to the enclosed drawings.

In the following, the principle according to the invention is described by referring to a flowchart shown in Fig. 2.

According to the present invention, the traffic carried in a media component is captured, instead of capturing the traffic carried in a PDP context. This can be effected in a GGSN, for example, since it handles the IP header of the user data.

Fig. 2 shows a flowchart of a procedure how the traffic carried in a media component is captured, i.e., how a packet of a media component are identified and provided to a Lawful Enforcement Agency (LEA) (as an example for an interception management element).

The procedure is started each time a packet arrives at the corresponding intercepting node (i.e., the GGSN in this example). In step S1, the packet is identified based on media component information contained in the packet header. Based on the media component information, it is checked whether this packet belongs to a session is

actually to be intercepted (step S2). If not, the procedure ends without performing any interception. If, however, it is determined that the particular packet is to be intercepted, the intercepted information is forwarded to an interception management element (step S3), such as a LEA (Law Enforcement Agency).

Thus, according to the invention the traffic carried in a media component is captured.

In the following, a first embodiment of the invention is described, in which the invention is described in more detail. In particular, two operations necessary for interception can be distinguished, namely activation of media component interception and provision of content of communications carried in media component. In the first embodiment, SIP is used as an example for a session protocol, and data is sent via packets using GPRS.

In the following, the activation of the media component interception is described. This has to be performed before the actual interception is carried out. In particular, in the activation some kind of information has to be obtained by which a packet of a media component to be intercepted can identified uniquely. Moreover, the network node(s) participating in the interception have to be activated (e.g., the GGSN).

There are two kinds of information elements by which a media component may be uniquely identified: IMS level session identification and media component identification associated with the former. That is, the media component information described above may comprise the IMS level session identification and the associated media component identification. An information element used to identify

IMS level session (i.e., which can be used as the IMS level session identification) can be a so-called Authorisation Token, as defined in 3GPP TS 29.207 V5.2.0 and TS 24.008 V5.6.0, for example, or ICID (IMS Charging Identifier), as defined in 3GPP TS 32.225 V5.2.0. The ICID is generated by the IMS node for a SIP session, and the value thereof is globally unique across all 3GPP IMS networks for a time period of at least one month, implying that neither the node that generated this ICID nor any other IMS node reuse this value before the uniqueness period expires. Hence, it can be used to reliably identify a particular multimedia component. According to the present embodiment, the Authorisation Token is used.

The media component identification as described above is associated to the IMS level session identification and uniquely identifies the media component within the session identified by the IMS level session identification. A flow identifier is defined in 3GPP TS 29.207 V5.2.0 (Annex C), for example, and is generally used for the identification of an IP flow within a media component associated with a SIP session. The flow identifier comprises the format of <Media component no, IP flow no>. According to the present embodiment, this flow identifier is used as a media component identification in interception activation. This type of media component identification is a control level identification and is referred to as control level media component identification in the following.

Alternatively, the media component information may comprise a user level identification, which is referred to as user level media component information in the following. The user level media component identification

may be an Ipv6 flow ID or the quintuple of IP source/destination address, TCP/UDP source/destination port and used protocol.

It is noted that the control level media component identification needs to be accompanied with the session identification in order to be unique, whereas the user level media component information does not need such a session identification.

The user level media component information can be referred to as network layer and/or transport layer information in user data. In provision of communication content, a media component may be identified by such network layer and/or transport layer information in user data. The network layer-only identification information is comprised of flow label field of IPv6 header (as defined in IETF RFC 2460, for example). The combined network layer and transport layer information is a combination of source address, destination address and protocol fields of IP header and source port and destination port fields of UDP (User Datagram Protocol) or TCP (Transmission Control Protocol) header (as defined in IETF RFC 768, RFC 793, respectively).

In the following, the activation of media component interception is described by referring to Figs. 3 and 4.

Fig. 3 illustrates the activation of interception of a media component MC2, whereas Fig. 4 illustrates the relevant signalling flow of the activation of the interception.

In detail, Fig. 3 shows a situation in which sessions of a user entity UE of a subscriber (e.g., subscriber A as

in Fig. 1) is to be intercepted. In this example it is assumed that the target UE shown in Fig. 3 performs two media sessions. That is, two media components MC1 and MC2 are to be considered, wherein only media component MC2 is to be intercepted. Comparing to the situation in Fig. 1, it is noted that the UE shown in Fig. 3 corresponds to UE B performing a first session with UE C (media component MC1, not to be intercepted) and a second session with UE A (media component MC2, to be intercepted).

The UE is connected to a SGSN, which in turn is connected to a GGSN. The GGSN is connected to a P-CSCF (Proxy CSCF). During the session establishment, the UE communicates with SIP protocol with CSCF (in this case P-CSCF). The GPRS network (SGSN and GGSN) provide the transport of the SIP messages. SIP protocol messages are carried in the signalling PDP context between SGSN and GGSN. Moreover, a secondary PDP context is established between SGSN and GGSN, which serves to carry user data that may have special requirements (e.g., Quality of Service (QoS) requirements). The secondary PDP context is not active during session establishment, but is created during the session establishment for user data. Alternatively only one general purpose PDP context may be used which carries both signalling and user data.

In addition, an ADMF (Administration Function) is provided which is adapted to receive information from the P-CSCF, for example, and to instruct other network elements (e.g., the GGSN) to carry out the interception. In particular, the ADMF receives media component information from the P-CSCF. The ADMF then sends a message to the GGSN regarding an interception activation on the media component MC2.

Moreover, also a DF3 (Delivery Function 3) is provided, by which during the interception the communication content (CC) data is forwarded to a LEMF (Law Enforcement Monitoring Facility), for example. During interception activation, the DF3 only receives an interception activation message from the ADMF (not shown in the figure).

The signalling flow during interception activation according to the first embodiment is described in the following by referring to the diagram shown in Fig. 4. It is noted that messages M1 to M11 refer to the normal session establishing procedure, whereas the messages M12 to M16 refer to the interception. Moreover, in this example it is assumed that the subscriber to be intercepted is originating a call.

During session establishment (i.e., after sending a SIP INVITE request to the CSCF in M1), an Authorisation Token is created for the session in PDF (as described in 3GPP TS 29.207 V5.2.0, for example). The Authorisation Token is delivered to UE (User Entity) in a 183 Session Progress SIP message (M2). The UE responses with a PRACK (Provisional Acknowledgement) message (M3), thereafter a further acknowledgment message is sent to the UE. It is noted that the flow identifiers may be carried in all of the messages M1 to M4. The messages M1 to M3 perform a handshaking process between P-CSCF and UE in which the media components parameters (codecs, delays, other parameters) are negotiated. Message M4 is an acknowledgement to the message M3.

In general, the flow identifiers are specified by the SDP (Session Description Protocol) descriptions that UE receives in INVITE, 183 Session Progress and PRACK

messages. In which messages the UE receives SDP descriptions depends on the role of the UE in session establishment (3GPP TS 24.228 V5.3.0, for example). All of the SIP messages are transferred in user plane of the GPRS.

At some point of the session establishment after the media component negotiation is finished (after receiving PRACK), it sends authorisation token, flow identifiers (alternatively SDP descriptions) and associated IMS identity to ADMF in message M12. In case it is decided that the session is actually to be intercepted, the interception is activated. In messages M13 and M14, the corresponding DF3 is activated. In messages M15 and M16, the ADMF requests GGSN to activate media component interception based on authorisation token and appropriate flow identifier. In detail, the main content in messages M13 and M15 is the media component information, which the GGSN and the DF3 need for the interception, and an LIID (Lawful Interception ID) that uniquely define the interception within the intercepting network.

After the session originating UE and a session terminating UE (i.e., the called user identity) have agreed on media components, they perform resource reservation in GPRS. This is performed in messages M5 to M11. Authorisation token and flow identifiers are passed from the UE to the GGSN via SGSN in GPRS control plane message Activate PDP Context Request (M5) and Create PDP Context Request (M6). Besides, it is noted that an Information element in Create PDP Context Request that carries authorisation token and flow identifiers is TFT (Traffic Flow Template, as defined in 3GPP TS 29.060 V5.5.0 and TS 24.008 V5.6.0, for example).

The GGSN then performs media authorisation with PDF and learns the relationships between user plane and control plane identification of media components. This is effected in messages M7 to M9, wherein in M7 a COPS (Common Open Policy) REQ (request) message is sent to the CSCF, by means of which the GGSN issues a configuration request, e.g., for establishing a media component. In message M8, the CSCF responds with a COPS DEC (decision) message, i.e., acknowledges that the request is granted. When the GGSN is ready, it sends a COPS REPT message to the CSCF (M9). In message M10, a corresponding Create PDP contest response is sent to the SGSN, and in message M11, a corresponding Activate PDP context response is sent to the UE. After this, the normal SIP connection is set up, which is indicated in Fig. 4 by a corresponding block.

As described above, by the COPS REQ and COPS DEC messages M7 and M8, media component information is exchanged between the P-CSCF and the GGSN. That is, in this messages the relevant information for identifying a session to be intercepted are contained.

It is noted that according to the present embodiment, the message M12, by which the activation of the interception is started, is sent after the P-CSCF has sent the COPS DEC to the GGSN in message M8. However, the message M12 can be sent to an arbitrary point of time after the media component negotiation is finished (messages M1 to M4). That is, for example, the message M12 can be sent immediately after the P-CSCF has sent the acknowledgement message M4, which would be the earliest point of time. Alternatively, the message M12 may be sent after the P-CSCF has received the COPS REPT message M9. When doing this, it is made sure that the GGSN is ready and that the session is actually going to be carried out.

Because in provision of content of communications the identification of a media component is done by using information in headers in user plane data, GGSN can use authorisation token and flow identifiers (which are control plane information, as described above) only during interception activation. GGSN performs the actual interception activation based on user level media component information contained in headers in user plane data.

Next, the provision of Content of Communications carried in the media component is described.

According to the present embodiment, the implementation of content of communication provision is rather straightforward. When the GGSN notices that a packet belongs to an intercepted media component, it duplicates the packet and forwards the duplicate (i.e., the CC data) to DF3 (message M17). The DF3 forwards the CC data to the LEMF in message M18. As stated earlier, the GGSN notices that a packet belongs to a certain media component by examining the network/transport layer headers in the user data and compares them to the user level identification of the media component.

Fig. 5 presents the provision of content of communications carried in the media component MC2. The configuration of Fig. 5 is the same as that of Fig. 3. In this example, the two sessions of the subscriber (UE) are established, such that a media component MC1 and a media component MC2 are sent by the GGSN to two different receiver. In this case, only the media component MC2 is intercepted and forwarded to the DF3.

Next, a second embodiment of the invention is described.

According to the second embodiment, the implementation of media component interception is eased such that the interception activation and provision may exploit current solutions. Instead of directly activating the interception using media component information, as described in connection with the first embodiment, it is activated using either user identification (e.g. IMSI) or PDP context identification (e.g. GPRS Charging ID) and the unwanted data is filtered out.

This requires that in addition to the authorisation token, flow identifiers and associated IMS identity, the ADMF receives also the GPRS Charging IDs of each PDP context used in IMS level session. ADMF can then directly activate interceptions for each PDP context or use the GPRS charging IDs to resolve the IMSI before performing the IMSI activation. If filtering is to be done in GGSN or in SGSN the media component information needs to be delivered to the intercepting node (i.e., GGSN or SGSN) with the interception activation request. If the filtering is done in DF3 (Delivery Function 3) the media component information needs to be delivered to it.

The media component information needs to be user level information in the implementation alternative using filtering. According to the second embodiment, the media component information have to be user level media component information because SGSN and DF3 by default do not have access to control level media component information, unlike the GGSN has.

The provision of content of communication is done in following way. The intercepting node examines the GTP

header of a packet and checks whether the IMSI or GPRS Charging ID found in the header is intercepted. If it is and only if it is, the IP and transport layer information is compared to user level media component information. In this way, the unwanted data is filtered out based on the user level media component information.

As mentioned above, this filtering can be done either in the intercepting node or in DF3 (Delivery Function 3).

The latter case is illustrated in Fig. 6. The structure is similar to that of Fig. 3 or 5, with the exception that now the PDP context is forwarded to the DF3. As mentioned above, the PDP context comprises both media components MC1 and MC2, of which only MC2 is to be intercepted. Thus, the DF3 filters the media component MC1 out, as mentioned above, so that only MC2 is provided to the LEMF.

Thus, the filtering approach according to the second embodiment is easy to implement, and it is advantageous that this approach can also be carried out in the SGSN.

The invention is not limited to the embodiments described above but can vary within the scope of the claims.

For example, the above embodiments can be freely combined. For example, depending on the load of the interceptin node and/or network, the filtering according to the second embodiment may be carried out additionally.

Moreover, the use of GPRS is only an example. The invention can be applied to any packet based communication system in which an interception can be carried out.

Furthermore, according to the first embodiment, control level media component information are used during the interception activation whereas according to both the first and the second embodiment user level media component information are used to filter out the unwanted data. However, also according to the first embodiment user level media component may be used during the interception activation, and also according to the second embodiment, control level media component information may be used. This, however, may depend on the particular situation, i.e., whether the intercepting node (e.g., SGSN or GGSN) is able to handle the particular type of media component information.

CLAIMS

1. A method for intercepting sessions, comprising the steps of

identifying (S1, S2) a packet of a session to be intercepted based on media component information of the session, and,

if the packet to be intercepted is identified, providing (S3) duplicated packets of the session to an interception management element.

2. The method according to claim 1, wherein the media component information comprises a multimedia level session identification and a control level media component identification associated to the multimedia level session identification.

3. The method according to claim 2, wherein the multimedia level session identification comprises an authorisation token.

4. The method according to claim 2, wherein the multimedia level session identification comprises a multimedia charging identifier.

5. The method according to claim 2, wherein the control level media component identification comprises a flow identifier.

6. The method according to claim 1, wherein the media component information comprises user level media component information.

7. The method according to claim 1, further comprising the step of

activating the interception, which is performed before the identifying step and in which the media component information are obtained from a session initiating procedure in which a target to be intercepted is participating.

8. The method according to claim 7, wherein in the activating step, the media component information are obtained from user plane data.

9. The method according to claim 8, wherein the media component information are obtained from session establishing messages (M1 to M4).

10. The method according to claim 1, wherein in the providing step data not to be intercepted is filtered out.

11. The method according to claim 10, wherein the data not to be intercepted is a media component not belonging to the session to be intercepted.

12. The method according to claim 10, wherein the filtering is performed based on media component identification or charging identifiers.

13. A system for intercepting sessions comprising an intercepting node and an intercepting management element, wherein

the intercepting node is adapted to identify a packet of a session to be intercepted based on media component information of the session, and to provide duplicated packets of the session to the interception

management element if the packet to be intercepted is identified.

14. The system according to claim 13, wherein the media component information comprises a multimedia level session identification and a control level media component identification associated to the multimedia level session identification.

15. The system according to claim 14, wherein the multimedia level session identification comprises an authorisation token.

16. The system according to claim 14, wherein the multimedia level session identification comprises a multimedia charging identifier.

17. The system according to claim 14, wherein the control level media component identification comprises a flow identifier.

18. The system according to claim 13, wherein the media component information comprises user level media component information.

19. The system according to claim 13, further comprising an interception activation element which is adapted to activate the interception wherein the media component information are obtained from a session initiating procedure in which a target to be intercepted is participating.

20. The system according to claim 19, wherein the activation element is adapted to obtain the media component information from user plane data.

21. The system according to claim 20, wherein the activation element is adapted to obtain the media component information from session establishing messages (M1 to M4).

22. The system according to claim 13, further comprising a filter element which is adapted to filter out data not to be intercepted.

23. The system according to claim 22, wherein the data not to be intercepted is a media component not belonging to the session to be intercepted.

24. The system according to claim 22, wherein the filter element is adapted to filter out based on media component identification or charging identifiers.

25. The system according to claim 22, wherein the filter element is included in the intercepting node.

26. The system according to claim 22, wherein the filter element is a node separated from the intercepting node.

ABSTRACT

The invention proposes a method for intercepting sessions, comprising the steps of identifying (S1, S2) a packet of a session to be intercepted based on media component information of the session, and, if the packet to be intercepted is identified, providing (S3) duplicated packets of the session to an interception management element.

(Fig. 2)

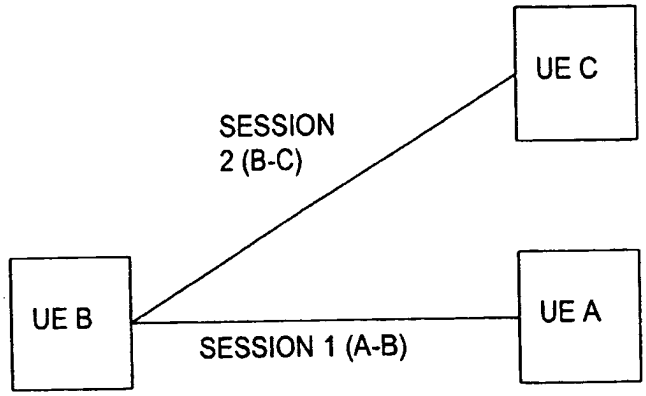


Fig. 1

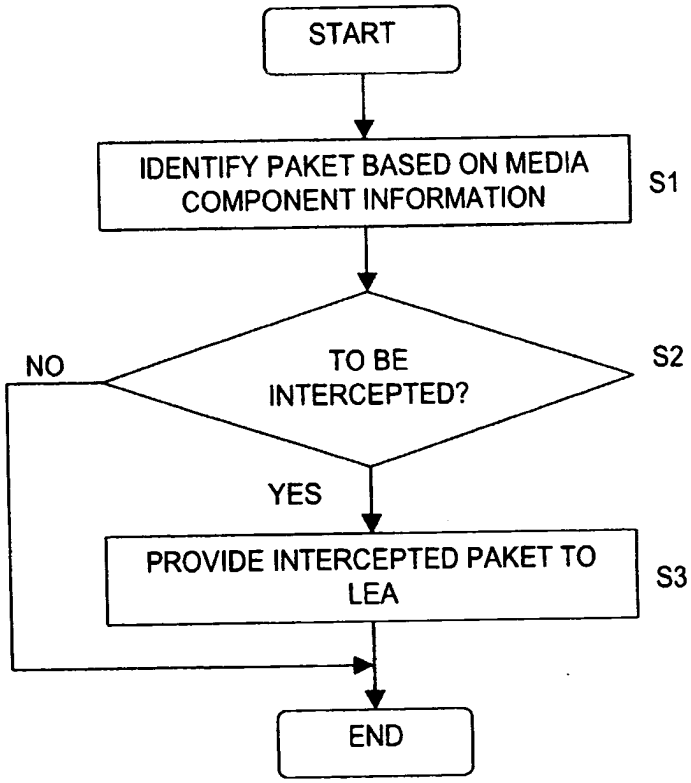


Fig. 2

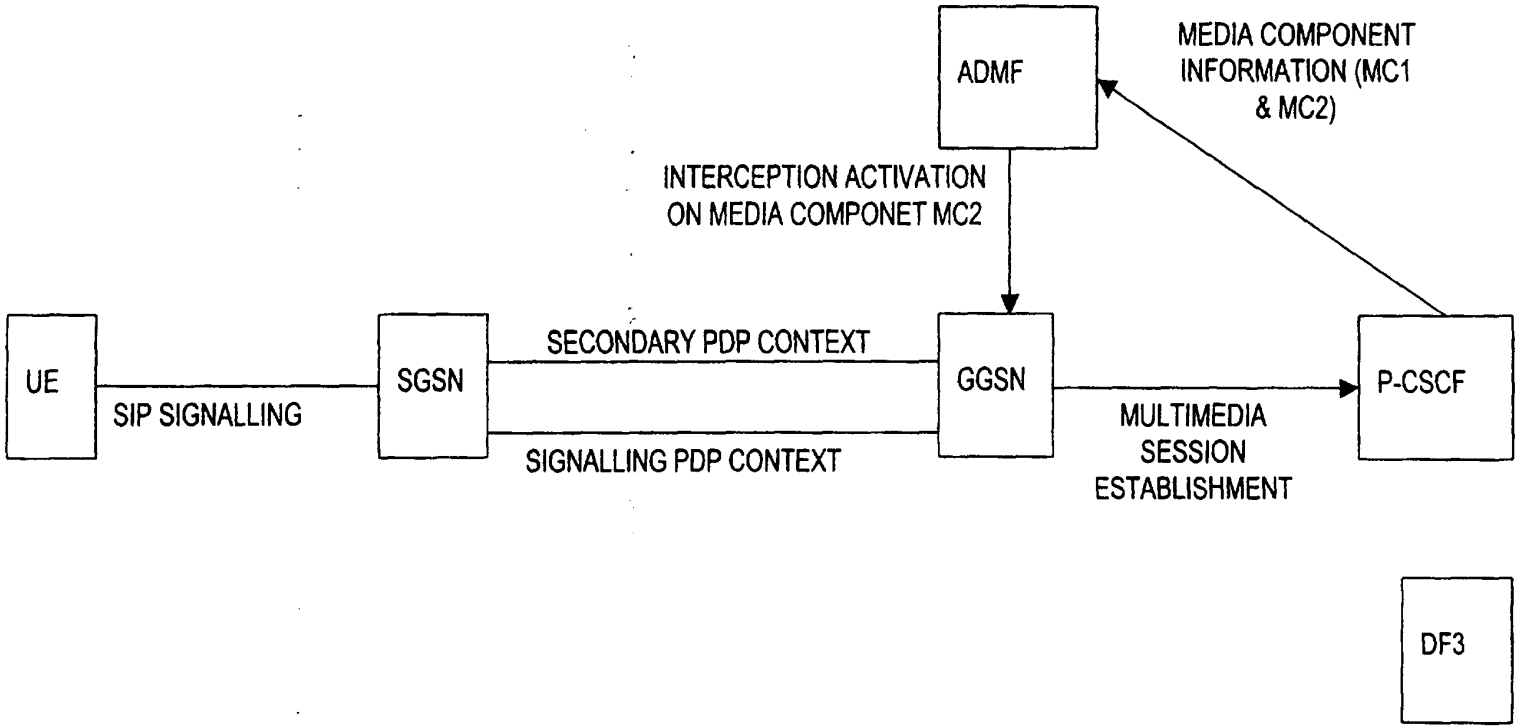

ADMF
MEDIA COMPONENT INFORMATION (MC1 & MC2)
INTERCEPTION ACTIVATION ON MEDIA COMPONET MC2
UE
SIP SIGNALLING
SGSN
SECONDARY PDP CONTEXT
SIGNALLING PDP CONTEXT
GGSN
MULTIMEDIA SESSION ESTABLISHMENT
P-CSCF
DF3

Fig. 3

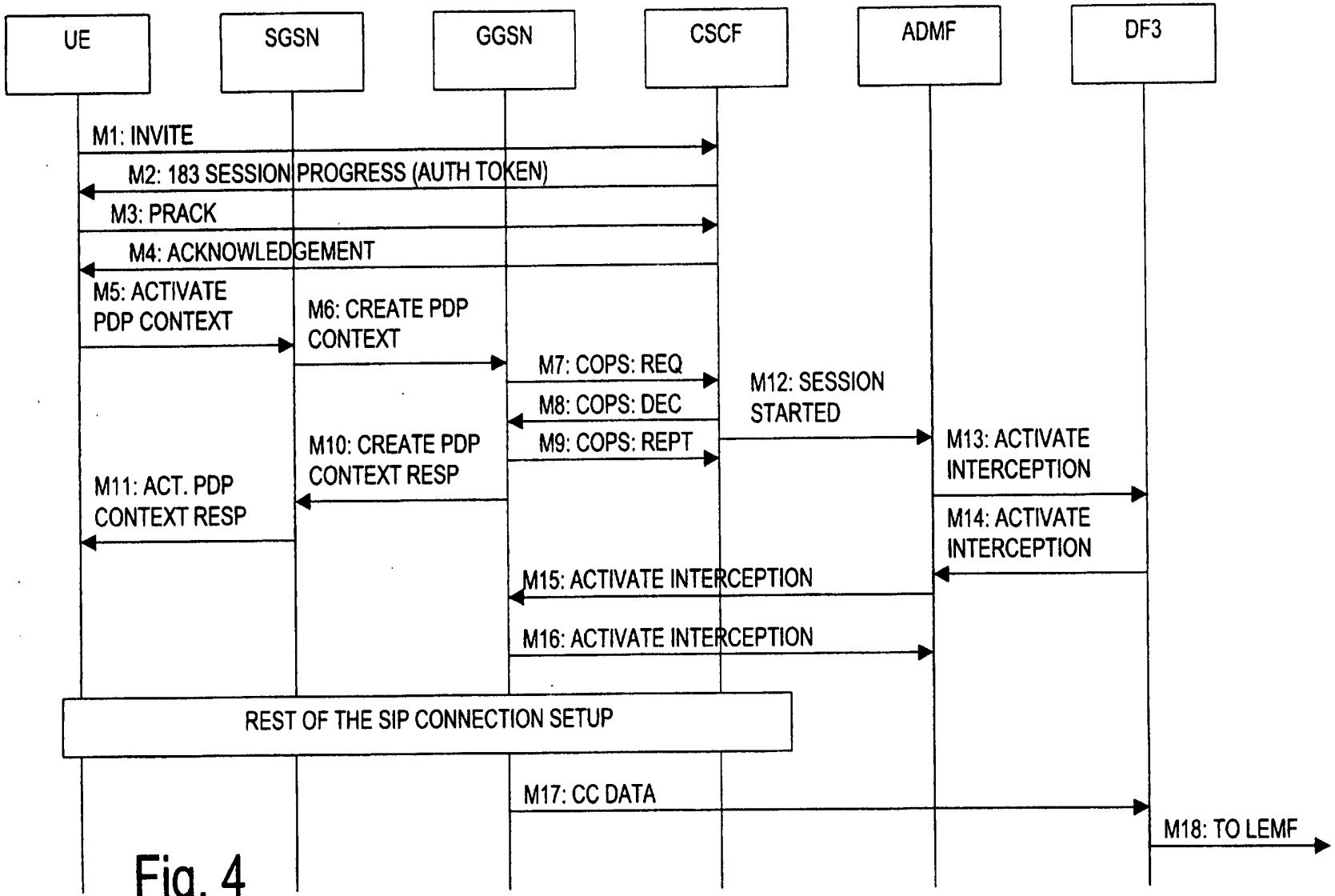

UE
SGSN
GGSN
CSCF
ADMF
DF3
M1: INVITE
M2: 183 SESSION PROGRESS (AUTH TOKEN)
M3: PRACK
M4: ACKNOWLEDGEMENT
M5: ACTIVATE PDP CONTEXT
M6: CREATE PDP CONTEXT
M7: COPS: REQ
M8: COPS: DEC
M9: COPS: REPT
M10: CREATE PDP CONTEXT RESP
M11: ACT. PDP CONTEXT RESP
M12: SESSION STARTED
M13: ACTIVATE INTERCEPTION
M14: ACTIVATE INTERCEPTION
M15: ACTIVATE INTERCEPTION
M16: ACTIVATE INTERCEPTION
REST OF THE SIP CONNECTION SETUP
M17: CC DATA
M18: TO LEMF

Fig. 4

315

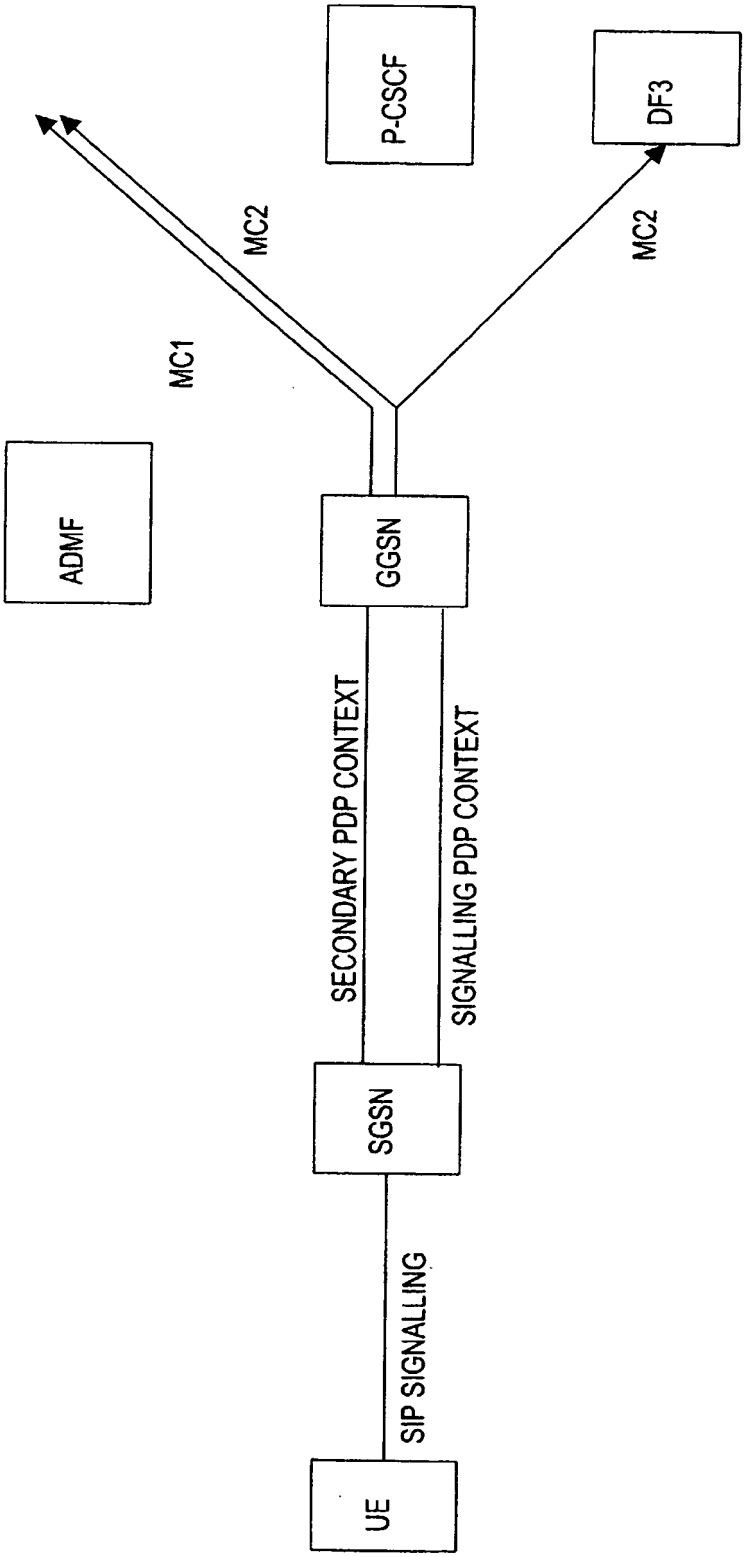

ADMF
MC1
MC2
P-CSCF
MC2
DF3
GGSN
SECONDARY PDP CONTEXT
SIGNALLING PDP CONTEXT
SGSN
SIP SIGNALLING
UE

Fig. 5

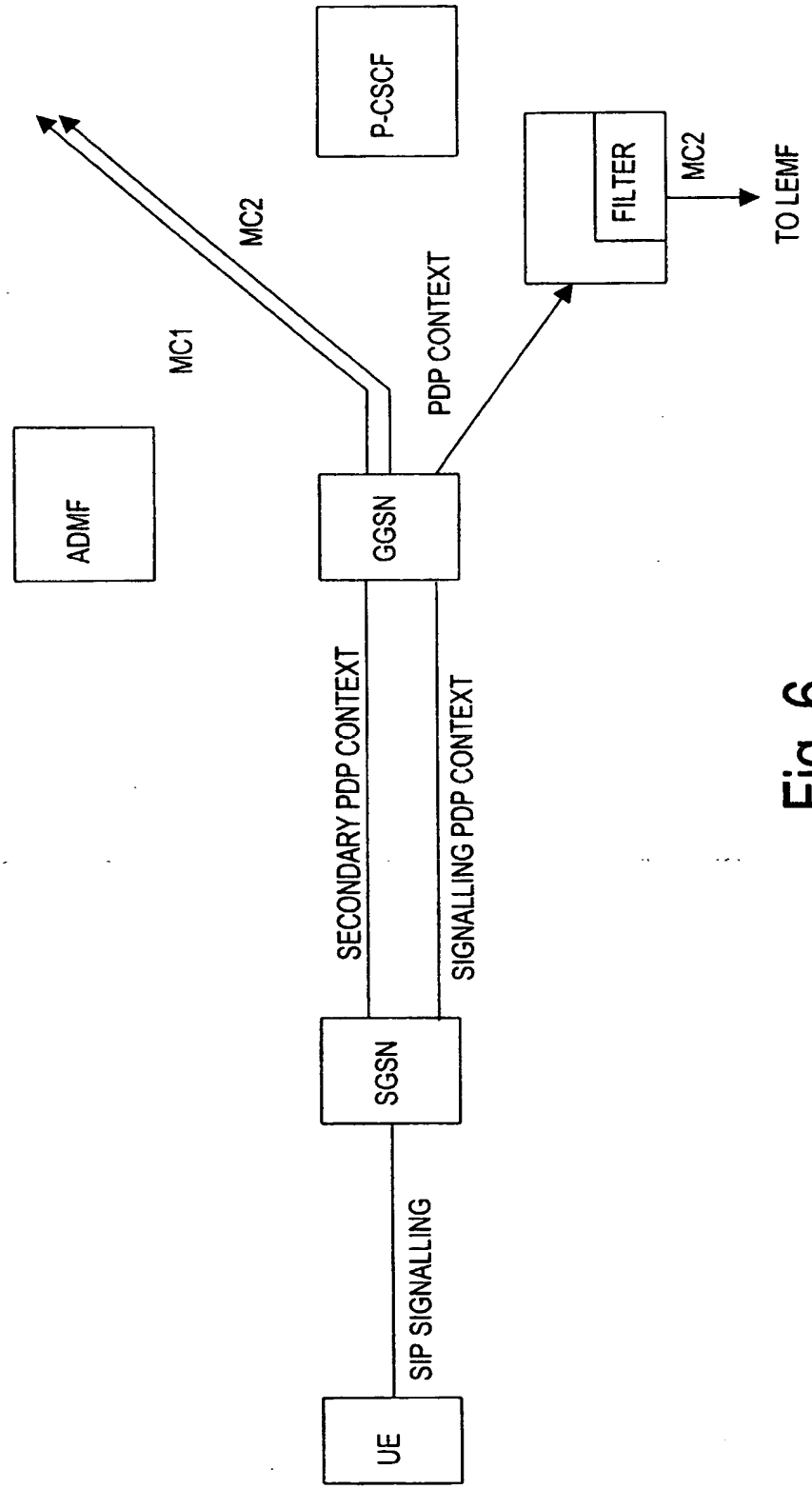

UE
SIP SIGNALLING
SGSN
SECONDARY PDP CONTEXT
SIGNALLING PDP CONTEXT
GGSN
ADMF
MC1
MC2
P-CSCF
PDP CONTEXT
FILTER
MC2
TO LEMF

Fig. 6